(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
21 février 2002 (21.02.2002)

PCT

(10) Numéro de publication internationale
WO 02/15133 A1

(51) Classification internationale des brevets[7] : G07F 7/08

(21) Numéro de la demande internationale :
PCT/FR01/02455

(22) Date de dépôt international : 26 juillet 2001 (26.07.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0010553 11 août 2000 (11.08.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : GEMPLUS [FR/FR]; Avenue Pic De Bertagne, Parc D'activités De Gemenos, F-13881 Gemenos (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : ROUSSEAU, Ludovic [FR/FR]; Bât A Les Aires St Michel, F-13400 Aubagne (FR).

(74) Mandataire : AIVAZIAN, Denis; c/o GEMPLUS, Av Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 GEMENOS (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

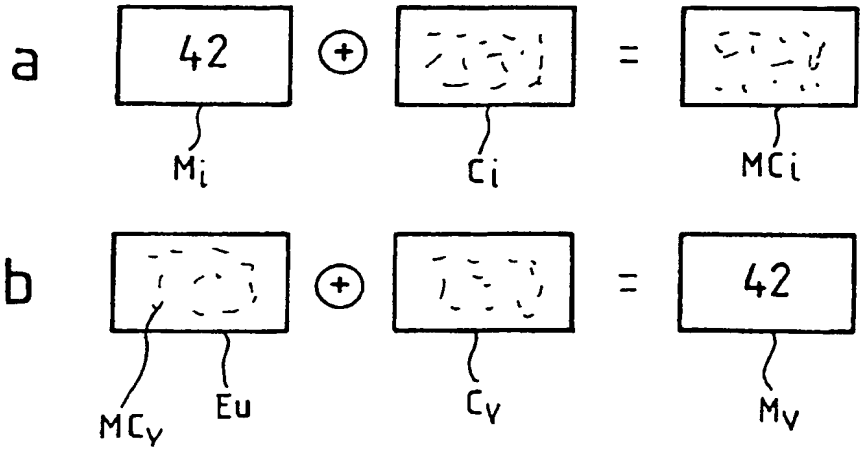
(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :
— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE,*

[Suite sur la page suivante]

(54) Title: SMART CARD MODULE DESIGNED TO EXCHANGE A MESSAGE WITH THE MODULE USER

(54) Titre : MODULE DE CARTE A PUCE APTE A ECHANGER UN MESSAGE AVEC L'UTILISATEUR DU MODULE



(57) Abstract: The invention concerns a microprocessor smart card module (10) designed to exchange a message M with the module user, comprising means for graphic encoding of said message with a computer mask.

(57) Abrégé : Un module 10 de carte à puce à microprocesseur apte à échanger un message M avec l'utilisateur du module, comprend des moyens de codage graphique dudit message par un masque informatique.

WO 02/15133 A1

DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

MODULE DE CARTE A PUCE APTE A ECHANGER UN MESSAGE AVEC L'UTILISATEUR DU MODULE

L'invention concerne un module de carte à puce à microprocesseur apte à échanger un message avec l'utilisateur de ce module.

L'invention concerne également un système incluant un tel module et un masque de décodage.

L'invention a également pour objet un procédé d'utilisation d'un tel module.

Le domaine de l'invention est celui de la cryptographie visuelle appliquée à la sécurisation d'une communication entre une carte à puce à microprocesseur notamment les cartes de paiement, et son utilisateur.

La carte à puce peut être une carte à contact et/ou sans contact.

La chaîne de communication entre une carte et son utilisateur n'est pas toujours sûre.

En effet, lorsque par exemple un utilisateur utilise une carte de paiement chez un commerçant, la transaction s'effectue à travers un terminal avec lequel la carte communique. Ce terminal sera dénommé dans la suite terminal lecteur de carte à puce. Le commerçant saisit un montant sur le clavier du terminal lecteur de carte à puce. Ce lecteur affiche ce montant sur son écran d'affichage. En cas d'accord sur le montant, l'utilisateur valide la transaction de débit en saisissant sur le terminal lecteur de carte à puce,

le code secret de sa carte. Le terminal lecteur de carte à puce envoie alors à la carte des informations de transaction incluant ce montant complété du code et d'autres informations transparentes pour l'utilisateur, notamment des informations identifiant le commerçant. La carte crypte alors l'ensemble de ces informations (signe la transaction), et envoie via le terminal lecteur de carte à puce, ce cryptogramme au serveur distant chargé de virer le montant, du compte bancaire de l'utilisateur vers celui du commerçant.

Dans le cas d'une carte de type porte-monnaie électronique, la carte elle-même dispose d'un certain crédit. Le montant est directement débité de la carte ; il n'y a pas de serveur distant.

Mais dans un cas comme dans l'autre, l'utilisateur n'a aucun contrôle sur ce qui est échangé entre la carte et le terminal lecteur de carte à puce. Ce que le terminal lecteur de carte à puce affiche peut ne pas correspondre à ce qui sera envoyé à la carte : le terminal lecteur de carte à puce peut afficher un montant et demander à la carte d'en débiter un autre ou enregistrer le code secret et demander par exemple à la carte de débiter plusieurs fois le même montant en lui fournissant plusieurs fois le code secret.

On a pris le paiement comme exemple mais on peut généraliser le problème à toute transaction basée sur un échange entre la carte et son utilisateur.

L'invention a pour but que la transaction soit validée par l'utilisateur de façon sécurisée et que cette validation ne soit valable que pour une seule transaction, c'est-à-dire que la communication entre la

carte et l'utilisateur via un terminal lecteur de carte à puce non sécurisé, soit elle-même sécurisée.

La carte doit pouvoir émettre une information secrète à destination de l'utilisateur, telle que seul l'utilisateur puisse prendre connaissance de cette information. De plus, cette information ne doit pas être modifiée par les intermédiaires entre la carte et l'utilisateur, sans que cette modification ne soit détectée par l'utilisateur.

Les problèmes de sécurisation dans le domaine des cartes à puce à microprocesseur sont souvent résolus en faisant appel à des calculateurs cryptographiques plus performants dans le domaine des calculs que le cerveau humain. En revanche, le système visuel humain est plus performant que les calculateurs dans le domaine de la reconnaissance de forme.

L'inventeur a ainsi appliqué au problème posé la méthode de cryptographie visuelle décrite dans l'article "Visual Cryptography" de M. Naor et A. Shamir présenté à la conférence EuroCrypt'94. Le problème considéré par ces auteurs est de coder un support écrit en noir et blanc d'une manière parfaitement sûre et telle que le support puisse être décodé directement par le système visuel humain sans calculs cryptographiques. La solution proposée consiste à considérer une page imprimée de texte chiffré en noir et blanc et un support transparent imprimé en noir et blanc également qui est la clé secrète. Le texte original est révélé en superposant le support transparent avec sa clé sur la page de texte chiffré alors que chacun des supports ne peut être différencié d'un bruit aléatoire.

L'invention a pour objet un module de carte à puce à microprocesseur apte à échanger un message avec l'utilisateur du module, principalement caractérisé en ce qu'il comprend des moyens de codage graphique dudit message par un masque informatique.

Selon une caractéristique de l'invention, le module comprend en outre un générateur de nombre aléatoire et des moyens d'association d'un tel nombre au message à coder.

Selon une autre caractéristique de l'invention, le module comprend des moyens d'ajout d'un bruit aléatoire au message codé.

Le module étant apte à être relié à un écran, il comprend avantageusement des moyens de commande de l'affichage du message codé sur ledit écran et éventuellement des moyens de commande de l'affichage du message codé à des endroits aléatoires de l'écran.

Selon une caractéristique de l'invention, le message étant un texte alphanumérique, le module comprend des moyens de commande de l'affichage à l'écran du message codé, selon différentes polices de caractères.

La carte à puce peut être une carte de type porte-monnaie électronique.

L'invention concerne également un dispositif de sécurisation d'un message entre un module de carte à puce à microprocesseur et son utilisateur, caractérisé en ce qu'il comprend un module tel que décrit précédemment et un masque de décodage dont dispose l'utilisateur, ledit masque de décodage, représentation visuelle du masque informatique sur un support

translucide, permettant de déchiffrer visuellement le message codé.

Le masque de décodage peut être constitué de plusieurs sous-masques.

Le module peut être intégré dans un corps de carte à puce ainsi que le masque de décodage.

L'invention concerne aussi un système de sécurisation d'un message entre un module de carte à puce à microprocesseur et son utilisateur, caractérisé en ce qu'il comprend un dispositif tel que décrit précédemment et un écran d'affichage apte à afficher le message codé généré par le module.

Le masque de décodage est préférentiellement de même format que l'écran d'affichage.

L'invention concerne enfin un procédé de sécurisation de l'échange d'un message, entre un module de carte à puce à microprocesseur comprenant des moyens de codage graphique dudit message par un masque informatique, et l'utilisateur dudit module disposant lui-même d'un masque de décodage, représentation visuelle du masque informatique sur un support translucide, l'échange entre la carte à microprocesseur et l'utilisateur s'effectuant à travers un terminal lecteur de carte à puce disposant d'un écran d'affichage et d'un dispositif de saisie et apte à échanger avec le module de carte à microprocesseur des informations de transaction incluant ledit message, caractérisé en ce qu'il comprend les étapes suivantes :

a) le terminal lecteur de carte à puce envoie les informations de transaction au module,

b) le module extrait le message des informations de transaction,

c) le module transforme le message en une image codée et commande l'affichage de ladite image codée sur l'écran du terminal lecteur de carte à puce,

d) l'utilisateur superpose le masque de décodage sur l'image codée affichée sur l'écran pour déchiffrer le message,

e) en cas d'accord sur le montant, l'utilisateur valide le montant et le module lance la transaction, annule la transaction sinon.

L'étape e) peut être remplacée par les étapes suivantes :

e) en cas d'accord sur le montant, l'utilisateur valide le montant sur le dispositif de saisie du terminal qui transmet cette validation au module, sinon l'utilisateur annule la transaction,

f) en cas de validation, le module lance la transaction et donne la preuve de la transaction au terminal lecteur de carte à puce, annule la transaction sinon.

L'étape suivante peut être insérée après l'étape b) :

le module génère une suite aléatoire N de caractères alphanumériques et l'associe au message,

et les étapes c) à f) remplacées par les étapes suivantes :

c) le module transforme le message auquel la suite N a été associée, en une image codée et commande

l'affichage de ladite image codée sur l'écran du terminal lecteur de carte à puce,

d) l'utilisateur superpose le masque de décodage sur l'image affichée sur l'écran pour déchiffrer la suite N et le message,

e) en cas de lisibilité de la suite N et d'accord sur le montant, l'utilisateur saisit la suite N sur le dispositif de saisie du terminal qui transmet N au module, sinon l'utilisateur annule la transaction,

f) le module compare la suite N reçue avec la suite N envoyée,

g) en cas de concordance, le module lance la transaction et donne la preuve de la transaction au terminal lecteur de carte à puce, annule la transaction sinon.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description faite à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

les figures 1a) et 1b) illustrent sur un exemple le principe de l'invention,

la figure 2 est la table de vérité de la fonction XOR que l'on obtient par la superposition des deux supports,

les figures 3a), 3b) sont les tables de vérité représentant la superposition de deux points respectivement noirs ou blancs, ou colorés selon un mode de réalisation de l'invention,

la figure 4 représente un terminal lecteur de carte à puce,

la figure 5 représente un schéma d'une carte à puce à microprocesseur.

L'exemple représenté sur les figures 1a) et 1b) illustre le principe du codage et du décodage d'un montant M, en l'occurrence le nombre "42".

Lorsque le commerçant a saisi le montant M sur le terminal lecteur de carte à puce, le terminal affiche ce montant sur un écran du terminal lecteur de carte à puce afin que le commerçant puisse vérifier que le montant affiché correspond bien à ce qu'il a saisi sur le terminal lecteur de carte à puce. Le terminal lecteur de carte à puce envoie alors à la carte les informations de transaction contenant le montant M. On distingue deux composantes pour M : sa représentation informatique Mi et sa représentation visuelle Mv telle qu'elle apparaît sur l'écran d'affichage du terminal lecteur de carte à puce.

Comme représenté figure 1a), la carte applique une clé de chiffrement Ci au montant Mi. Dans la suite, on entendra par carte, le module comportant la puce de circuit intégré. La clé de chiffrement consiste en un codage graphique sous forme informatique que l'on appellera masque informatique Ci : il s'agit d'une répartition tirée au hasard de points de deux couleurs différentes. La représentation visuelle de ce masque informatique Ci est un masque Cv.

En appliquant sous forme informatique le masque Ci au montant Mi, la carte transforme ainsi Mi en un message codé MCi et commande l'affichage de l'image de MCi sur l'écran du terminal lecteur de carte à puce.

Cette image apparaît sous forme d'une répartition MCv de points de deux couleurs différentes. Finalement, le message codé MCv est le masque Cv sur lequel certains points ont été inversés, c'est-à-dire sont passés d'une couleur à l'autre. Les points inversés sont ceux de la représentation graphique du montant M, c'est-à-dire de Mv. Visuellement, l'image MCv se présente également sous la forme d'une répartition aléatoire de points de deux couleurs différentes. L'écran sur lequel s'affiche le message codé MCv peut être différent de l'écran d'affichage destiné à l'usage du commerçant; le terminal lecteur de carte à puce dispose alors de deux écrans d'affichage, l'un pour l'affichage en clair du montant destiné au commerçant, l'autre pour l'affichage du message codé destiné à l'utilisateur. On note Eu l'écran destiné à l'utilisateur.

Comme représenté figure 1b), l'utilisateur superpose alors sur l'image MCv qui s'affiche sur l'écran Eu, un masque de décodage correspondant au masque Cv imprimé sur un support translucide : la superposition du masque de décodage Cv sur le message codé MCv révèle la forme "42" du montant M d'origine, c'est-à-dire Mv.

Le masque Cv peut lui-même résulter de la superposition de plusieurs sous-masques.

Les superpositions indiquées sur les figures 1a) et 1b) par le signe + dans un cercle, sont représentées par la fonction "ou exclusif" aussi notée XOR, dont la table de vérité est représentée figure 2. En superposant comme représenté figure 3a), des supports en noir et blanc, un point noir étant représenté par

"1", un point blanc ou transparent par "0", on obtient le résultat escompté sauf pour la superposition de deux points noirs pour laquelle on obtient un point noir, alors que l'on souhaite obtenir un point blanc. Ce problème est résolu dans l'article "Visual Cryptography" en particulier en augmentant le nombre de points.

Selon un mode de réalisation de l'invention, les couleurs cyan et magenta disponibles sur la plupart des écrans d'affichage actuels ont été choisies pour résoudre ce problème.

Comme représenté figure 3b), deux points cyan C superposés donnent un point cyan C ; deux points magenta M superposés donnent un point magenta M ; un point cyan C superposé à un point magenta M donne un point bleu foncé BF. Le résultat de la table de vérité de la figure 2) est ainsi obtenu en considérant que "1" est représenté par le bleu foncé BF qui est opaque, et que "0" est représenté par le cyan C ou le magenta M qui sont des couleurs claires. Ces couleurs ont été choisies pour obtenir le meilleur contraste possible entre les points représentés par les points cyan ou magenta d'une part et les points bleus foncés d'autre part.

D'autres couleurs peuvent être envisagées.

Selon ce mode de réalisation de l'invention, le terminal lecteur de carte à puce dispose d'un écran Eu capable d'afficher des points cyan et magenta. Le message codé MCv affiché sur l'écran Eu apparaît à l'utilisateur sous forme d'une répartition de points

cyan et magenta. Mais lorsque l'utilisateur, muni d'un support translucide Cv imprimé de points cyan et magenta applique ce support Cv sur l'écran Eu, la forme Mv représentant le montant M apparaît en bleu foncé sur un fond de points cyan et magenta.

Le support Cv de l'utilisateur et l'écran Eu du terminal lecteur de carte à puce sont de préférence de même format pour faciliter la superposition des points du support Cv sur les points de l'écran Eu.

Le procédé selon l'invention comprend les étapes suivantes :

1- le terminal lecteur de carte à puce T représenté figure 4, envoie à la carte à microprocesseur les informations de transaction qui contiennent le montant M de la transaction,

2- la carte génère une suite aléatoire N de caractères alphanumériques, par exemple un nombre aléatoire N sur 4 chiffres décimaux,

3- la carte crée une image en associant le nombre N au montant M et transforme cette image sur laquelle le nombre N est par exemple juxtaposé au montant M, en une image codée ou message codé Mci ;

4- la carte commande l'affichage de ladite image codée MCi sur l'écran Eu du terminal T lecteur de carte à puce,

5- l'utilisateur vérifie avec le masque de déchiffrement Cv le montant M de la transaction et lit le nombre N proposé par la carte et associé au montant M (N apparaît par exemple sur le côté de M),

6- en cas d'accord sur le montant M, l'utilisateur entre la valeur N sur le dispositif S de saisie du terminal lecteur de carte à puce,

7- le terminal lecteur de carte à puce transmet la valeur N à la carte,

8- la carte vérifie que la valeur N reçue correspond à la valeur N qu'elle a générée,

9- en cas de concordance, la carte lance la transaction selon la procédure habituellement utilisée et donne la preuve de transaction au terminal lecteur de carte à puce.

Le nombre N utilisé par ce procédé se substitue au code secret habituellement saisi par l'utilisateur sur le terminal lecteur de carte à puce. On peut en effet omettre la procédure relative au nombre N et valider le montant par le code secret (étape 6 et suivantes) selon la pratique courante. Mais contrairement au code secret qui ne varie pas et que le terminal pourrait enregistrer et réutiliser frauduleusement, le nombre N varie à chaque transaction et ne peut donc être réutilisé par le terminal lecteur de carte à puce.

Selon ce procédé, l'utilisateur peut vérifier le montant M et ne donner son accord que si le montant M reçu par la carte est le bon montant.

De plus, selon ce procédé, on peut empêcher une fraude par laquelle lors d'une transaction, le terminal lecteur de carte à puce affiche une image codée frauduleusement mémorisée, correspondant à une transaction précédente de l'utilisateur, à la place de l'image codée générée par la carte pour cette transaction.

Par exemple, on suppose que le terminal lecteur de carte à puce a déjà effectué avec l'utilisateur une transaction d'un montant M assorti d'un nombre aléatoire N, selon le procédé de l'invention.

L'utilisateur fait ensuite une nouvelle transaction pour le même montant M.

Une fraude peut consister pour le terminal lecteur de carte à puce :

- à envoyer un autre montant M' à la carte, qui va effectuer les étapes 2 à 4 du procédé de l'invention. Elle va notamment générer un nouveau nombre aléatoire N' pour cette nouvelle transaction et créer une image codée correspondante Mci', correspondant à M' et N'.

- à faire afficher sur l'écran Eu du terminal T lecteur de carte à puce l'image codée Mci de la première transaction (M,N), (que le terminal lecteur de carte à puce aura frauduleusement mémorisée), à la place de l'image codée Mci' envoyée par la carte.

L'utilisateur ne peut pas voir la fraude, car avec le masque de déchiffrement, il va voir le bon montant M. Il va donc valider la nouvelle transaction, en entrant le nombre aléatoire N, selon le procédé de l'invention.

La carte va alors détecter qu'il n'y a pas concordance entre le nombre aléatoire N' qu'elle a proposé pour la deuxième transaction et le nombre N

qu'elle reçoit, et refuser d'effectuer la deuxième transaction.

Ce procédé permet ainsi d'assurer une authentification de l'utilisateur par la carte et un contrôle d'intégrité graphique du message par l'utilisateur.

Le codage graphique du message est réalisé par la carte à microprocesseur. On a représenté sur la figure 5 le schéma fonctionnel d'une carte à microprocesseur susceptible de mettre en œuvre le codage graphique.

La carte à microprocesseur comporte une unité centrale 1 qui exécute les instructions des programmes stockés dans une mémoire 2 de type ROM, une mémoire de travail 3 de type RAM, des mémoires permanentes 4 de type EEPROM et bien sûr une interface d'entrée-sortie 5. Les programmes d'application sont souvent stockés dans ces mémoires 4. Un générateur 6 de nombre aléatoire est associé à l'unité centrale. Le masque Ci peut aussi être réalisé par ce générateur et changer à chaque transaction ou être mis en mémoire 2 voire en mémoire 4.

Ces divers éléments de la carte sont regroupés dans un module 10, généralement intégré dans un support plastique 20.

Le masque Cv dont dispose l'utilisateur de la carte pourra être intégré au support 20. Cette disposition est d'autant plus adaptée pour une carte fonctionnant en mode sans contact. Mais pour accomplir l'étape 5 du procédé dans le cas d'une carte fonctionnant en mode à contact, l'utilisateur peut éventuellement retirer la

carte à microprocesseur du terminal T dans lequel elle est insérée, pour pouvoir disposer du masque Cv. La carte peut aussi rester insérée dans le terminal T lorsque celui-ci comprend un écran placé par exemple sous le masque Cv de la carte lorsqu'elle est insérée.

La vérification accomplie, l'utilisateur réinsère la carte à microprocesseur dans le terminal T.

Mais le terminal lecteur de carte à puce connaissant le montant M, saisi par le commerçant par exemple et le message codé MCi ou MCv peut déduire le masque Ci.

Pour éviter que le terminal lecteur de carte à puce puisse déduire le masque Ci, une solution consiste à le changer à chaque transaction. Il faut alors que l'utilisateur change son masque Cv en conséquence. La sécurité assurée sera alors celle du masque jetable : elle sera maximale. Cette solution ne peut être envisagée si le masque Cv est intégré au support 20 notamment pour des raisons de coût.

Plusieurs solutions peuvent être envisagées pour limiter les connaissances que le terminal lecteur de carte à puce peut déduire.

La carte peut ajouter un bruit aléatoire au message codé transmis au terminal. Ce bruit généré par le générateur de nombre aléatoire 6 représenté figure 5, doit être suffisamment important pour brouiller le terminal lecteur de carte à puce mais suffisamment faible pour ne pas empêcher le système visuel humain de reconnaître la forme représentant le montant M.

Une autre solution consiste à ce que la carte commande que le montant M soit affiché sur l'écran Eu du terminal lecteur de carte à puce à des endroits choisis aléatoirement par le générateur 6.

Une troisième possibilité est que la carte change la police de caractères pour chaque montant M, de manière aléatoire. La carte disposera alors de plusieurs polices de caractères qui seront choisies aléatoirement par le générateur 6.

Bien sûr ces trois solutions peuvent être combinées.

REVENDICATIONS

1. Module (10) de carte à puce à microprocesseur apte à échanger un message (M) avec l'utilisateur du module (10), caractérisé en ce qu'il comprend des moyens de codage graphique dudit message (M) par un masque informatique (Ci).

2. Module (10) de carte à puce à microprocesseur selon la revendication précédente, caractérisé en ce qu'il comprend en outre un générateur de nombre aléatoire et des moyens d'association d'un tel nombre au message (M) à coder.

3. Module (10) de carte à puce à microprocesseur selon l'une des revendications précédentes, caractérisé en ce qu'il comprend des moyens d'ajout d'un bruit aléatoire au message codé.

4. Module (10) de carte à puce à microprocesseur selon l'une des revendications précédentes et apte à être relié à un écran (Eu), caractérisé en ce qu'il comprend des moyens de commande de l'affichage du message codé sur ledit écran (Eu).

5. Module (10) de carte à puce à microprocesseur selon la revendication précédente, caractérisé en ce qu'il comprend des moyens de commande de l'affichage du message codé à des endroits aléatoires de l'écran (Eu).

6. Module (10) de carte à puce à microprocesseur selon l'une des revendications 4 à 5, le message (M) étant un texte alphanumérique, caractérisé en ce qu'il comprend des moyens de commande de l'affichage à l'écran (Eu) du message codé, selon différentes polices de caractères.

7. Module (10) de carte à puce à microprocesseur selon l'une des revendications précédentes, caractérisé en ce que la carte à puce est une carte de type porte-monnaie électronique.

8. Dispositif de sécurisation d'un message (M) entre un module (10) de carte à puce à microprocesseur et son utilisateur, caractérisé en ce qu'il comprend un module conforme à l'une des revendications précédentes et un masque de décodage (Cv) dont dispose l'utilisateur, ledit masque de décodage (Cv) étant une représentation visuelle du masque informatique (Ci) sur un support translucide, permettant de déchiffrer visuellement le message codé.

9. Dispositif de sécurisation d'un message selon la revendication précédente, caractérisé en ce que le masque de décodage (Cv) est constitué de plusieurs sous-masques.

10. Dispositif de sécurisation d'un message selon la revendication 8, caractérisé en ce que le module est intégré dans un corps (20) de carte à puce et en ce que

le masque de décodage (Cv) est également intégré audit corps (20) de la carte à puce.

11. Système de sécurisation d'un message (M) entre un module (10) de carte à puce à microprocesseur et son utilisateur, caractérisé en ce qu'il comprend un dispositif selon l'une des revendications 8 à 10 et un écran d'affichage (Eu) apte à afficher le message codé généré par le module (10).

12. Système de sécurisation selon la revendication précédente, caractérisé en ce que le masque de décodage (Cv) est de même format que l'écran (Eu) d'affichage.

13. Procédé de sécurisation de l'échange d'un message, entre un module de carte à puce à microprocesseur comprenant des moyens de codage graphique dudit message par un masque informatique, et l'utilisateur dudit module disposant lui-même d'un masque de décodage, représentation visuelle du masque informatique sur un support translucide, l'échange entre la carte à microprocesseur et l'utilisateur s'effectuant à travers un terminal lecteur de carte à puce disposant d'un écran d'affichage et d'un dispositif de saisie et apte à échanger avec le module de carte à microprocesseur des informations de transaction incluant ledit message, caractérisé en ce qu'il comprend les étapes suivantes :

a) le terminal lecteur de carte à puce envoie les informations de transaction au module,

b) le module extrait le message des informations de transaction,

c) le module transforme le message en une image codée et commande l'affichage de ladite image codée sur l'écran du terminal lecteur de carte à puce,

d) l'utilisateur superpose le masque de décodage sur l'image codée affichée sur l'écran pour déchiffrer le message,

e) en cas d'accord sur le montant, l'utilisateur valide le montant et le module lance la transaction, annule la transaction sinon.

14. Procédé de sécurisation de l'échange d'un message selon la revendication précédente, caractérisé en ce que l'étape e) est remplacée par les étapes suivantes :

e) en cas d'accord sur le montant, l'utilisateur valide le montant sur le dispositif de saisie du terminal qui transmet cette validation au module, sinon l'utilisateur annule la transaction,

f) en cas de validation, le module lance la transaction et donne la preuve de la transaction au terminal lecteur de carte à puce, annule la transaction sinon.

15. Procédé de sécurisation de l'échange d'un message selon la revendication 13, caractérisé en ce que l'étape suivante est insérée après l'étape b):

le module génère une suite aléatoire N de caractères alphanumériques et l'associe au message,

et en ce que les étapes c) à f) sont remplacées par les étapes suivantes :

c) le module transforme le message auquel la suite N a été associée, en une image codée et commande l'affichage de ladite image codée sur l'écran du terminal lecteur de carte à puce,

d) l'utilisateur superpose le masque de décodage sur l'image affichée sur l'écran pour déchiffrer la suite N et le message,

e) en cas de lisibilité de la suite N et d'accord sur le montant, l'utilisateur saisit la suite N sur le dispositif de saisie du terminal qui transmet N au module, sinon l'utilisateur annule la transaction,

f) le module compare la suite N reçue avec la suite N envoyée,

g) en cas de concordance, le module lance la transaction et donne la preuve de la transaction au terminal lecteur de carte à puce, annule la transaction sinon.

FIG_1a

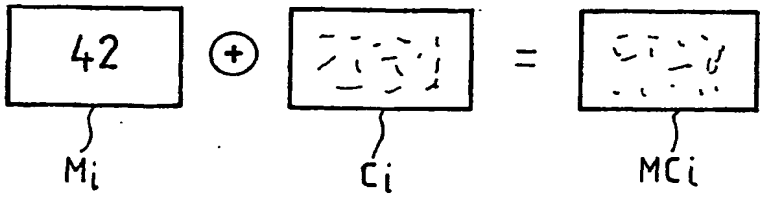


FIG_1b

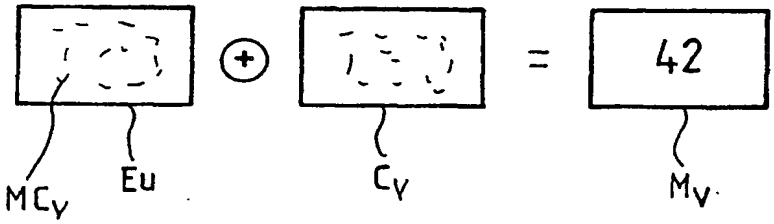


FIG_2

A \ B	1	0
1	0	1
0	1	0

FIG_3a

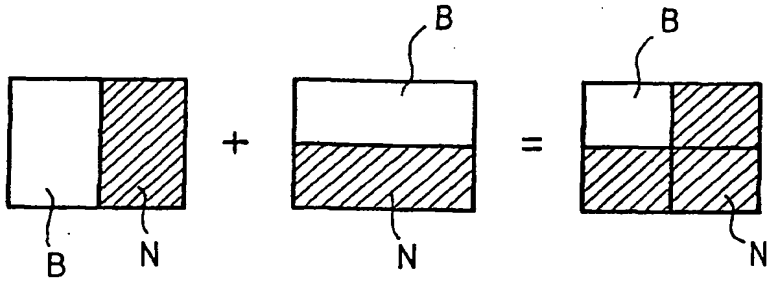


FIG_3b

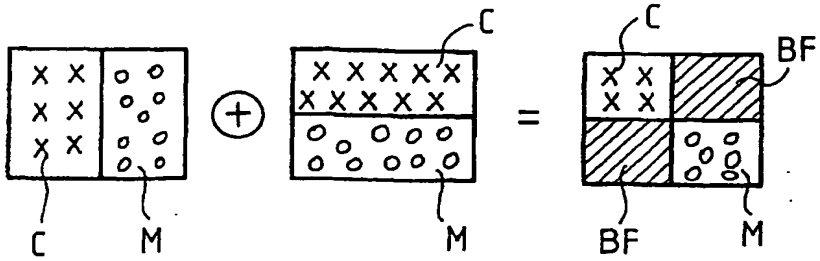


FIG_4

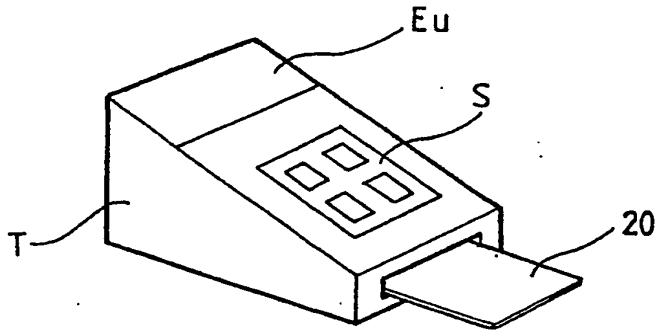
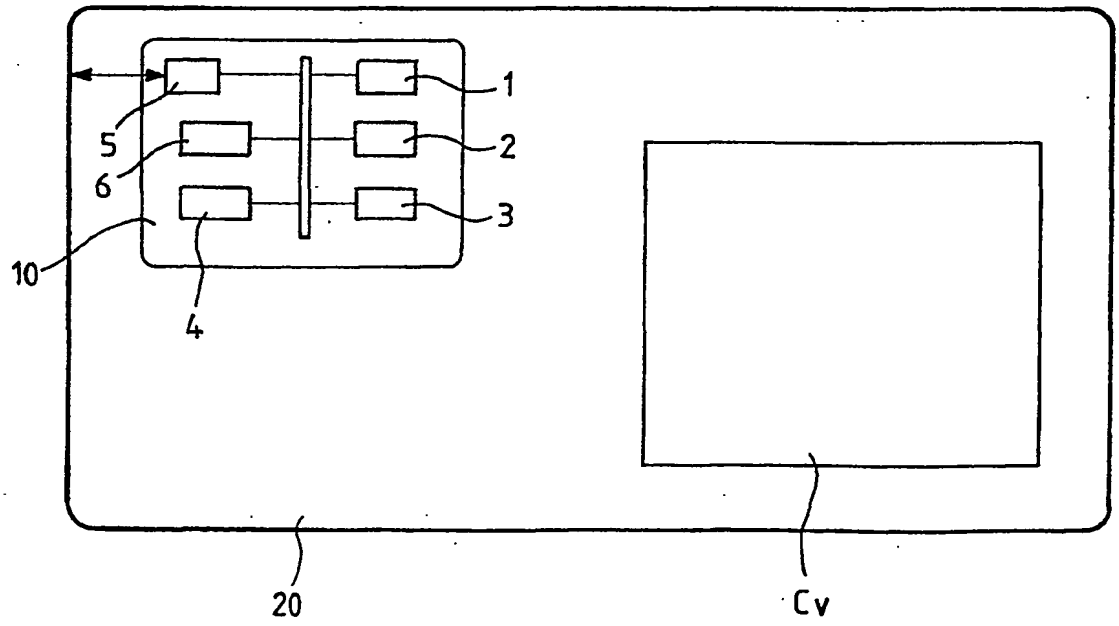


FIG_5



INTERNATIONAL SEARCH REPORT

	al Application No
	PCT/FR 01/02455

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 032 859 A (HUGHES MICHAEL ET AL) 7 March 2000 (2000-03-07) the whole document	1,13
A	US 5 907 142 A (KELSEY CRAIG E) 25 May 1999 (1999-05-25) the whole document	1,13
A	EP 0 256 768 A (OKI ELECTRIC IND CO LTD) 24 February 1988 (1988-02-24) the whole document	1,13

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 October 2001	30/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Degraeve, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

In ial Application No
PCT/FR 01/02455

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 6032859	A	07-03-2000	NONE		
US 5907142	A	25-05-1999	NONE		
EP 0256768	A	24-02-1988	JP	2096562 C	02-10-1996
			JP	7104891 B	13-11-1995
			JP	63039099 A	19-02-1988
			DE	3789179 D1	07-04-1994
			DE	3789179 T2	07-07-1994
			EP	0256768 A2	24-02-1988
			HK	38495 A	24-03-1995
			KR	9108452 B1	15-10-1991
			US	4877947 A	31-10-1989

RAPPORT DE RECHERCHE INTERNATIONALE

D ternationale No
PCT/FR 01/02455

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, IBM-TDB, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 032 859 A (HUGHES MICHAEL ET AL) 7 mars 2000 (2000-03-07) le document en entier	1,13
A	US 5 907 142 A (KELSEY CRAIG E) 25 mai 1999 (1999-05-25) le document en entier	1,13
A	EP 0 256 768 A (OKI ELECTRIC IND CO LTD) 24 février 1988 (1988-02-24) le document en entier	1,13

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
16 octobre 2001	30/10/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Degraeve, A

RAPPORT DE RECHERCHE INTERNATIONALE

	rnationale No
	PCT/FR 01/02455

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 6032859	A	07-03-2000	AUCUN		
US 5907142	A	25-05-1999	AUCUN		
EP 0256768	A	24-02-1988	JP	2096562 C	02-10-1996
			JP	7104891 B	13-11-1995
			JP	63039099 A	19-02-1988
			DE	3789179 D1	07-04-1994
			DE	3789179 T2	07-07-1994
			EP	0256768 A2	24-02-1988
			HK	38495 A	24-03-1995
			KR	9108452 B1	15-10-1991
			US	4877947 A	31-10-1989